Illinois Tollway

CURRENT EMPLOYMENT OPPORTUNITIES
QUALIFICATION SHEET

This position is currently vacant within the Tollway.
The Human Resources Section will accept applications, with resumes from:

May 8, 2013 through May 22, 2013
****

DEPARTMENT	POSITION	SALARY
Information Technology	Security Administrator	$51,490.00 - $117, 243.00/Year (G-6)

JOB QUALIFICATIONS:
To be selected for a position, an applicant must (1) meet the minimum requirements of the job posting, (2) pass a written exam (if applicable), (3) satisfy a background check (which may be extensive), (4) pass an oral interview, during which the interviewer(s) will further evaluate the applicant's qualifications and (5) provide certified transcripts, certifications, and/or license upon candidate processing and/or transfer, if the position requires a degree, certification, and/or license.
Internal Applicants who are current employees must have worked in their current position long enough to pass probation to be eligible to apply for the position. In addition, applicants are also subjected to an internal investigation which includes an evaluation of their work record, safety and discipline records, their performance assessments and time and attendance records (including late starts and early quits) for the preceding 12 months. (Authorized absences will not be included for purposes of assessing whether attendance is satisfactory.)

EDUCATION:
- BS or BA degree in computer science or related field preferred; or equivalent work experience in an Information Security management role.

EXPERIENCE
- Two to four years experience with encryption technologies to provide data security.

THE FOLLOWING SKILLS AND ABILITIES ARE REQUIRED/DESIRED:
- Knowledge at the proficient level of current techniques and hardware/software capabilities of a large-scale, multi-location database and communications environment.
- Ability to understand and clearly relate to other members of the organization, technical manuals, software specifications, hardware principals of operations, and general methods of systems software and security.
- Thorough understanding of the build procedures, operating systems, database and programming languages used by the department. (MCP, UNIX, Windows , LINC, Oracle, Access, SMTP and TCP/IP).
- Must be detail oriented, analytical and highly organized, and be able to handle a variety of tasks in an efficient manner.
- Excellent written/oral communication and interpersonal skills are required.
- CISSP or PCI QSA certified or working towards certification preferred.
- A main function of this position is to conduct site inspections at various Tollway facilities during regular work hours as well as subject to being "on-call". This is accomplished by incumbent use of a vehicle to travel to and from respective sites. Additionally reports to Central Administration as necessary. Visits of Tollway facilities may include meeting with Tollway employees and/or contractors. Therefore, a Valid Drivers License is required.
- Must be able to lift 50 pounds
- Must have the ability to work overtime as required including during off hours / holidays / weekends
- Must participate in 24x7x365 scheduled support rotation
- Must carry Tollway issued cellphone for on-call support and for response to calls/incidents before or after shift hours / weekends / holidays.
- Salaried position and not eligible for overtime.

Ways to apply
- **Online:** Complete the Illinois Tollway application, save it to the computer and email it to jobs@getipass.com
- **In person:** Submit the completed application or pick up and complete the application at Illinois Tollway Headquarters located at 2700 Ogden Avenue in Downers Grove between 8:00 a.m. and 4:30 p.m., Monday through Friday.
- **By mail:** Send the completed application to:
  Illinois Tollway – Human Resources
  2700 Ogden Avenue
  Downers Grove, IL 60515

This position may be subject to Random Selection. Random Selection Interview Policy Link

Application Link
All applications must be received by the application deadline indicated on the qualification sheet or Internet site

POSITION PURPOSE:

The incumbent is responsible for data security daily duties including the administration, maintenance and monitoring of security measures, which safeguard access to enterprise computing and network equipment as well as corporate files and data elements.

The incumbent works with the IT Security Manager to administer, monitor and maintain system security policies. Recognizes and identifies potential areas where existing data security policies and procedures require change, or where new ones need to be developed.

The incumbent is responsible for monitoring the data security environment including establishing and receiving automated alerts, reviewing logs and reporting issues to executive management.

The incumbent is responsible to maintain compliance with all required security standards including Payment Card Industry Standards (PCI). Incumbent is responsible to assist with the planning, design and implementation of security enhancements required to maintain PCI compliance as compliance requirements evolve and advance.

The incumbent is responsible to assist with maintaining a comprehensive enterprise security plan. The plan will include provisions and recommendations for keeping the security environment current with developing and advancing technologies required to ensure the safety of corporate computing equipment, software and data.

NATURE AND SCOPE:

The Security Administrator reports directly to the IT Security Manager. Based on the functions of the Security Administrator position the incumbent will have access to sensitive and confidential information and must exercise discretion and maintain confidentiality at all times.

The incumbent has the challenge of protecting enterprise information assets while minimizing the impact upon those who need legitimate business access to the data.

The incumbent is responsible for helping to maintain the overall enterprise security of all aspects of the Authority's computing environment. This requires mid level knowledge of operating systems, systems applications, data and networks. This includes UNIX/Linux, Windows, Active Directory, Cisco & F5 Security Appliances, Tripwire Enterprise & Log Center, Nessus, Trend and an understanding of Oracle/SQL database environments. A thorough knowledge of the Internet, SMTP and TCP/IP communication protocols is also required.

Responsibilities include maintaining standards, documentation, procedures and security awareness training to control information security activities throughout the Authority, ensuring the safety and protection of information system assets. Ensures protection of information system assets from loss, disclosure or fraudulent manipulation. Provides assistance with investigation, coordination, reporting and follow up of computer network security incidents.

This responsibility includes assisting with coordinating the design, development, maintenance, and testing of the overall security plans for each critical functional area of the organization.

Routinely monitors systems and network for possible security problems on a daily basis. Audits network security logs to ensure compliance is being enforced.

Maintains contact with vendors regarding security system updates and technical support of security products. Makes recommendations and implements changes to

NATURE AND SCOPE (Continued)

work methods and procedures to make them more effective and/or to strengthen
security measures.

Performs vulnerability scanning and risk analysis for enterprise functional areas to identify security
vulnerabilities and perform risk mitigation as required.

Routine contact is required with other IT managers and staff personnel at all organizational levels to assist
with development, implementation, maintenance and enforcement of security methods and measures.

REQUIREMENTS:

BS or BA degree in computer science or related field preferred; or equivalent work experience in an
Information Security management role. Two to four years experience with encryption technologies to
provide data security. Knowledge at the proficient level of current techniques and hardware/software
capabilities of a large-scale, multi-location database and communications environment. Ability to
understand and clearly relate to other members of the organization, technical manuals, software
specifications, hardware principals of operations, and general methods of systems software and security.
Thorough understanding of the build procedures, operating systems, database and programming
languages used by the department. (MCP, UNIX, Windows , LINC, Oracle, Access, SMTP and TCP/IP).
Must be detail oriented, analytical and highly organized, and be able to handle a variety of tasks in an
efficient manner. Excellent written/oral communication and interpersonal skills are required.

CISSP or PCI QSA certified or working towards certification preferred.

A main function of this position is to conduct site inspections at various Tollway facilities during regular
work hours as well as subject to being "on-call". This is accomplished by incumbent use of a vehicle to
travel to and from respective sites. Additionally reports to Central Administration as necessary. Visits of
Tollway facilities may include meeting with Tollway employees and/or contractors. Therefore, a Valid
Drivers License is required.

Must be able to lift 50 pounds
Must have the ability to work overtime as required including during off hours / holidays / weekends
Must participate in 24x7x365 scheduled support rotation
Must carry Tollway issued cellphone for on-call support and for response to calls/incidents before or after
shift hours / weekends / holidays.
Salaried position and not eligible for overtime.

PRINCIPLE ACCOUNTABILITIES:

1. Maintains and monitors all log-on identifications and access rules, defining specific access to network,
files and database management systems.

2. Perform other daily, quarterly and annual duties as required by PCI.

3. Management of external vendors that are contracted to perform vulnerability analysis, scanning and
pen testing against Authority systems.

4. Works with the IT Security Manager to develop, produce and maintain system security policies.
Recognizes and identifies potential areas where existing data security polices and procedures require
change, or where new ones need to be developed.

PRINCIPLE ACCOUNTABILITIES (Continued):

5. Participates in the Change Management process for all systems and applications for the movement of test systems to production. Works with the implementation review board for the approval of changes applied to system software and database software submitted by the applications development and technical support groups.

6. Trains users in the application of all Authority security policies and assist with awareness programs.

7. Assist with PCI Administration for IT and vendor systems.

8. Assist with preparation and data gathering for annual security assessments that are performed by external vendors, this includes PCI and general security audits.

9. Other duties as assigned.